IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

SUSAN NIEBLAS, individually and on behalf her daughter "JANE DOE", a minor, and on behalf of all others similarly situated, Plaintiffs, v. MANAGED CARE OF NORTH AMERICA, INC., MCNA INSURANCE COMPANY, and MCNA HEALTH CARE HOLDINGS, INC., Defendants.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs Susan Nieblas and her minor daughter "Jane Doe" (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, bring this data breach Class Action Complaint against Defendants Managed Care of North America, Inc., MCNA Insurance Co., and MCNA Health Care Holdings, Inc. (collectively, "Defendants" or "MCNA") and allege, upon personal knowledge as to their own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. MCNA touts itself as a "leading dental benefits manager committed to providing high quality services to state agencies and managed care organizations for their Medicaid, Children's Health Insurance Program ("CHIP"), and Medicare members."[1] MCNA serves over 5

[1] https://www.mcna.net/en/company-overview

million children and adults, and also offers dental plans for private employers, individuals and families. *Id.*

2. In the ordinary course of business Defendants collect, maintain, and store their customers' highly sensitive personally identifying information ("PII"), including Social Security numbers, dates of birth, full names, addresses, drivers' license numbers, health insurance information and telephone numbers, along with customer protected health information ("PHI"), including medical and laboratory testing, diagnosis and treatment information, as well as customer health insurance information.

3. MCNA states that it: "takes pride in the fact that we are recognized leaders in the dental benefits industry. One of our strengths is our ability to administer dental plans in an effective and innovative manner while safeguarding our members' protected health information. **We are committed to complying with the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We demonstrate our commitment through our actions.** " (Emphasis added).

4. Regarding PHI, MCNA states on its website: "In keeping with federal and state laws and our own policy, we have a responsibility to protect the privacy of your information. We have safeguards in place to protect your information in various ways."[2] With respect to customer PII, MCNA states that it "will not use or share your information other than as described here unless you tell us we can in writing."[3]

5. MCNA's "commitment through [its] actions" is plainly false -- as a direct and proximate result of Defendants' failure to implement reasonable security protections sufficient to prevent a foreseeable and avoidable ransomware cyberattack, on February 26, 2023, and lasting

[2] https://www.mcna.net/en/privacy
[3] *Id.*

until March 7, 2023, unauthorized actors compromised Defendants' network, accessed, and extracted highly-sensitive PII and PHI information of more than 8.9 million of MCNA's customer patients, including the Plaintiffs and putative Class Members ("the Data Breach").

6. Although Defendants became aware of the Data Breach on March 6, 2023, Defendants did not timely notify Plaintiffs and Class Members of the Data Breach and/or inform them that their PII and PHI was compromised until on or about May 26, 2023 (the "Notice Letter"), nearly two and a half months after the Data Breach occurred. Accordingly, Plaintiffs and Class Members were not aware that their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

7. Even more telling, on information and belief, the LockBit ransonware group, one of the world's most active ransomware groups, claimed responsibility for the Data Breach and leaked some of the stolen data on its dark web data leak site as proof of data theft, and demanded a $10 million ransom to prevent the publication of all of the stolen data. It appears that the ransom was not paid, as the group published the stolen files on April 7, 2023.

8. As a result, there is an increased and substantial risk that Plaintiffs and Class Members will experience an increased risk to the compromise of their PII and PHI.

9. Defendants disregarded Plaintiffs' and Class Members' rights by, among other things, intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII and PHI stored within Defendants' information system were protected and safeguarded against unauthorized access, misuse, and disclosure, failing to take basic industry-standard steps to prevent, identify, contain a breach of its system's security, failing to follow applicable, required and appropriate

protocols, policies and procedures regarding the encryption of data, even for internal use, and failing to give timely and adequate notice to Plaintiffs and Class Members that their PII and PHI had been subject to the unauthorized access of an unknown third party.

10. Plaintiffs and Class members suffered injuries as a result of Defendants' conduct including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their PII. These risks will remain for the lifetimes of Plaintiffs and the Class.

11. Accordingly, Plaintiffs bring this Class Action Complaint on behalf of all those similarly situated persons – the Class Members -- whose PII and PHI was compromised as a result of Defendants' negligence, violations of federal and state statutes, and on other grounds, in failing to: (i) adequately protect their PII and PHI; (ii) adequately warn them of Defendants' inadequate information security practices; (iii) adequately secure computer systems and hardware containing protected PII and PHI using reasonable and effective security measures free of vulnerabilities and incidents; and (iv) failure to timely warn them of the Data Breach.

12. Plaintiffs and the Class Members seek all available remedies, including but not limited to statutory and nominal damages, compensatory damages for identity theft, fraud, and time spent, reimbursement of out-of-pocket costs, adequate credit monitoring services funded by Defendants, and injunctive relief including improvements to Defendants' data security systems and practices to ensure they have reasonably sufficient security practices to safeguard their customers' PII and PHI that remains in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

13. Plaintiff Nieblas is and has been, at all relevant times, a resident and citizen of Idaho. Plaintiff Nieblas received a copy of the May 26, 2023, Notice Letter, via U.S. mail, from MCNA on or about June 13, 2023.

14. Plaintiff Nieblas provided her PII and PHI to Defendants in connection with dental insurance she received and provided that information on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable safeguards to protect that information. If Ms. Nieblas had known that Defendants would not adequately protect her PHI and PII, she would not have entrusted Defendants with that information and would have sought the services, including insurance, of other dental providers.

15. Plaintiff Jane Doe, a minor, is and has been, at all relevant times, a resident and citizen of Idaho. Plaintiff Jane Doe received the May 26, 2023 Notice Letter, via U.S. mail, from MCNA on June 13, 2023.

16. Jane Doe's mother, Plaintiff Neiblas, provided Jane Doe's PII and PHI to Defendants in connection with dental insurance they provided to her on the condition that it be maintained as confidential and with the understanding that Defendants would employ reasonable

safeguards to protect that information. If Jane Doe's legal guardian had known that Defendants would not adequately protect her minor child's PHI and PII, Ms. Nieblas could not have entrusted Defendants with that information and would have sought the services, including insurance, of other dental providers.

17. Defendant MCNA Insurance Company is a dental benefits manager with its principal place of business located at 3100 SW 145th Avenue, Suite #200, Miramar, FL 33027.

18. Defendant Managed Care of North America, Inc. is a dental benefits manager with its principal place of business located at 200 West Cypress Creek Road, Suite 500, Fort Lauderdale, FL 33309.

19. Defendant MCNA Health Care Holdings, LLC is the parent of MCNA Insurance Company and Managed Care of North America, Inc. with its principal place of business located at 200 West Cypress Creek Road, Suite 500, Fort Lauderdale, FL 33309.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

21. This Court has personal jurisdiction over Defendants because they operate and maintain their principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Defendants are authorized to and regularly conduct business in this District and make decisions regarding corporate governance and

management of their businesses in this District, including decisions regarding the security measures to protect its customer patients' PII and PHI.

22. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District, including decisions made by Defendants' governance and management personnel or inaction by those individuals that led to the Data Breach; Defendants are headquartered in this District; Defendants maintain Plaintiffs' and Class Members' PII PHI in this District; and Defendants caused harm to Plaintiff and Class Members from within this District.

STATEMENT OF FACTS

Background

23. MCNA is the largest dental insurer in the nation for government-sponsored Medicare/Medicaid and CHIP, with over five million members across eight states. MCNA Dental also offers dental plans and services for private employers, individuals, and families throughout the United States.

24. Plaintiffs and Class Members are current and former MCNA customer patients who obtained insurance from Defendants.

25. To obtain medical dental insurance from Defendants, Plaintiffs and Class Members were required to provide – and MCNA was required to collect and maintain -- sensitive and confidential PII and PHI, including customer patient names, Social Security numbers, health insurance information, and sensitive health care information, which MCNA stored and maintained in its computer systems. Indeed, by their nature MCNA's customer patient health testing, treating and insuring -- the PHI at issue is incredibly sensitive information.

26. Defendants tout on their website that they are technologically savvy and their

management information system, DentalTrac™ is "ensuring[ing] the security and availability of data through strict adherence to HIPAA requirements, keeping MCNA Dental in full compliance with all federal regulations."[4]

27. MCNA Dental's website also states that:

a) "MCNA has successfully completed an independent, third-party SOC 2 audit of the processes and controls that ensure the security and availability of our information management systems and data."

b) "DentalTrac™ is hosted across multiple geographically dispersed, military grade, secure, and state-of-the-art data centers. All hardware components are fully mirrored in every location guaranteeing high scalability and business continuity to support our current and future needs."

c) "The DentalTrac™ system has been based on HIPAA-compliant solutions. MCNA is fully committed to ensuring a clear and easy path to HIPAA readiness well ahead of federally mandated compliance deadlines."[5]

28. Defendants rely extensively on technology systems and networks to provide their services, along with their customer patients' PII and PHI which are critical to Defendants' core business operations.

29. Defendants use the PII and PHI they collect to create and maintain records stored in digital format on hardware, such as computers, mobile devices, flash drives, off-site "clouds" or similar storage devices and means, and that are transmitted, shared, or accessed through MCNA's networks.

30. By obtaining, collecting, storing, using, disseminating the PII and PHI they collect

[4] https://www.mcnala.net/en/company-overview
[5] https://www.mcna.net/en/technology/

from Plaintiffs and Class Members, Defendants derive substantial economic benefits. For example, Defendants gather, create, and distribute customer plaintiff health information as its customer patients authorize to doctors, nurses, technicians, staff, and other healthcare professionals who become involved in a customer patient's health care to provide, coordinate, or manage that patient's healthcare. Such data is a core part of MCNA's business operations. MCNA receives payment for the health care services it has provided and the related information and testing results (PII and PHI) obtained from or for the benefit of MCNA's customer patients' other health care providers for diagnosis and treatment.

HIPAA Requirements To Protect PII and PHI Data

31. Defendants are covered entities under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. Thus, HIPAA requires Defendants' "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

32. Defendants also are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

33. HIPAA and HITECH work in tandem to provide guidelines and rules for

maintaining protected health information. HITECH references and incorporates HIPAA.

34. HIPAA and HITECH obligated Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

35. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

36. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

37. HIPAA's Security Rule requires Defendants to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information; Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
c. Ensure compliance by its workforce.

38. HIPAA requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

39. Defendants also are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

40. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires

Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[5]

41. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

42. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

43. HIPAA requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[6] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[7]

44. In sum, HIPAA requires, among other things, that Defendants implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity

of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, et seq. Additionally, HIPAA requires that Defendants provide adequate and timely notification to every affected individual following the impermissible use or disclosures of any PHI. Individual notice must be provided to affected individuals without unreasonable delay. Further, for a breach involving more than 500 individuals such the Data Breach involving Defendants, entities are required to provide notice in prominent media outlets. *See* 45 CFR § 164.400, et seq.

45. In the ordinary course of their business as required by law, Defendants must provide every customer patient with a HIPAA compliant disclosure form in which they represent that they will protect patient customer PII and PHI, including that of Plaintiffs and Class Members.

FTC Requirements To Protect PII and PHI Data

46. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices to prevent data breaches. According to the FTC, the need for data security should be factored into all business decision- making.

47. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information.

48. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying

information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

49. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[9]

50. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[10] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[11]

51. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[12]

52. The FTC recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC's Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, et seq.

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

SOC 2 Type 2 Attestation Requirements

55. One of the services provided by auditors is to evaluate and report on a company's System and Organization Control ("SOC"). SOC reporting attests to whether the company has adequate controls relevant to its data security, data processing integrity of the systems it uses to process data, and the confidentiality and privacy of the information processed by these systems.

56. As stated on Defendants' website, "MCNA has successfully completed an independent, third-party SOC 2 audit of the processes and controls that ensure the security and availability of our information management systems and data."[6] Organizations like Defendants that would seek a SOC 2 attestation are typically looking for ways to build trust in their operations

[6] https://www.mcna.net/en/technology/

across current and future clients.

57. SOC 2 audits utilize AICPA's Trust Services Criteria (TSC) framework and its Trust Services Principles (TSP):

- **Security** – Prevention of unauthorized or harmful uses and disclosures of data;
- **Availability** – Accessibility of user-facing systems and information at all times;
- **Process Integrity** – Completeness, timeliness, and authorization of all processes;
- **Confidentiality** – Protection against breaches of legally protected information; and
- **Privacy** – Protection against breaches of personally identifiable information.

58. A SOC 2 attestation is a report on an organization's ability to ensure some combination of these principles to its clients. It may focus on all five or a selection thereof and is generated for a specialized audience.

59. Defendants' SOC attestation that their data systems and networks are adequate to protect the security of its customer patients' PII and PHI data were patently false.

Cyber Security Industry Standards To Protect PII and PHI Data

60. Cyber security industry experts routinely identify entities, like Defendants, in that collect, store and utilize PII and PHI as being particularly vulnerable to cyberattacks because of the tremendous value of that information to cyber criminals.

61. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of PII and/or PHI, like Defendants, including but not limited to:

- educating all employees;
- strong passwords;
- multi-layer security, including firewalls, anti-virus, and anti-malware software;
- encryption, making data unreadable without a key;
- multi-factor authentication; and
- backup data and limiting which employees can access sensitive data.

62. Other standard best cybersecurity industry practices that are applicable in the healthcare industry to entities such as Defendants that collect, store and utilize customer patient

PII and/or PHI include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points, as identified in part by the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

Defendants' Knowledge of HIPAA, FTC and Industry Standards & Representations To Plaintiffs and Class Members to Protect their PII and PHI Data

63. Defendants hold themselves out as respecting customer patients' privacy to gain the trust of its customer patients who use its products and services, including Plaintiffs and Class Members.

64. Defendants know, and are required to know, of HIPAA, FTC, and cyber security industry standards, guidelines and legal requirements to protect the PII and PHI of its customer patients, including Plaintiffs and Class Members, from such cyberattacks and data breaches.

65. Such knowledge is reflected in the fact that Defendants represent to their customer patients, including Plaintiffs and Class Members, that they will comply with PII and PHI data privacy and security requirements, including those implemented by HIPAA, the FTC, and industry standards regarding the protection of PII and PHI and prompt and adequate notification of data breaches.

66. Defendants directly and implicitly represented to its customer patients, including

Plaintiffs and Class Members, that the PII and PHI they provided to MCNA and/or that MCNA collected on their behalf for their benefit, including as a condition of submitting an application and other documentation for MCNA's health care and services and products, would be kept safe, confidential, and private and that MCNA would not permit the disclosure of such information to anyone other than whom Plaintiffs and Class Members explicitly authorized.

67. Defendants made express and implied representations concerning their commitment to user privacy, data security, and regulatory compliance that would lead a reasonable person in similar circumstances to believe that Defendants had, have, and will maintain in place reasonable cybersecurity practices and procedures to protect from unlawful use or disclosure of any customer patient's PII and PHI they collect or maintain in the regular course of business. Indeed, MCNA's Privacy Policy provides:

> **Notice of Privacy Practices**
>
> This notice describes how health information about you may be used and disclosed and how you can get access to this information. Please review it carefully. The privacy of your health information is important to us.
>
> This notice took effect 04/14/03. These privacy practices have been updated effective June 2018. They will remain in effect until they are changed. **This notice applies to all MCNA dental programs that are administered by Managed Care of North America, Inc. and MCNA Insurance Company.**
>
> What is MCNA's Legal Duty regarding the notice of privacy practices?
> The law says MCNA has to keep your health information private. We have to give you this notice about our privacy practices, our legal duties and your rights. We must follow the privacy practices that are in this notice. If needed, we can change the notice and the new one would apply to all health information we keep. If this happens, the new notice will be available upon request, posted on our website or we will send you a copy (electronically or through the mail). The changes must be within the law. The changes may apply to all of the old and new health information we have. Before we change our privacy practices, this notice will be changed.
>
> What is personal health information?
> Personal health information includes both medical information and individually identifiable information, like your name, address, telephone number, or Social Security

number. This information is created or received by a healthcare provider or health plan that relates to your physical or mental health or condition, providing healthcare to you, or the payment for such healthcare. We protect this information in all formats including electronic, written and oral information.

How do we protect your information?

In keeping with federal and state laws and our own policy, we have a responsibility to protect the privacy of your information. We have safeguards in place to protect your information in various ways including:

- Limiting who may see your information and how we use or disclose your information.
- Informing you of our legal duties about your information.
- Training our employees and associates about company privacy policies and procedures.[7]

68. In discussing the private and confidential nature of a patient's medical information and MCNA's requirement to maintain the privacy of protected health information ("PHI"), the following is provided (*see* https://www.mcna.net/en/privacy):

How can MCNA use or share my health information?

We are allowed or required to share your information in other ways. We have to meet many conditions in the law before we can share your information for these purposes below.

- Help with public health and safety issues
    - We can share health information about you for certain situations such as:
        - Preventing disease
        - Helping with product recalls
        - Reporting adverse reactions to medications
        - Reporting suspected abuse, neglect, or domestic violence
        - Preventing or reducing a serious threat to anyone's health or safety
- Do research
    - We can use or share your information for health research
- Comply with the law
    - We will share information about you if you state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we're complying with federal privacy law.

[7] https://www.mcna.net/en/privacy

- Address workers' compensation, law enforcement, and other government requests
    - We can use or share health information about you:
        - For workers' compensation claims
        - For law enforcement purposes or with a law enforcement official
        - With health oversight agencies for activities authorized by law
        - For special government functions such military, national security, and presidential protective services
- Respond to lawsuits and legal actions
    - We can share health information about you in response to a court or administrative order, or in response to a subpoena.
- Assist in disaster relief efforts
- Contact you with information about health-related benefits and services, appointment reminders, or about treatment alternatives that may be of interest to you if you have not opted out as described below.
- Share your information with your plan sponsor to permit them to perform plan administration functions such as eligibility, enrollment, and disenrollment activities. We will not share detailed health information with your plan sponsor unless you provide us your permission, or your plan sponsor has certified they agree to maintain the privacy of your information.
- Disclose your health information to a coroner or medical examiner. We may also disclose medical information to funeral directors consistent with applicable law to carry out their duties.
- We will never share your information for marketing purposes, sell your personal health information, or share most uses and disclosure of psychotherapy notes unless you give us written permission.

What are MCNA's responsibilities regarding my health information?

We are required by law to maintain the privacy and security of your protected health information. We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information. We must follow the duties and privacy practices described in this notice and give you a copy of it. We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

Plaintiffs And Class Members Provision of PII and PHI To Defendants

69. Plaintiffs and Class Members value the privacy and confidentiality of their Private Information and take reasonable steps to protect and maintain the confidentiality of their own PII

and PHI.

70. Plaintiffs and Class Members were required to provide to Defendants, and/or permit Defendants to acquire, their PII and PHI in order to obtain the medical and laboratory services and products that MCNA offers.

71. Plaintiffs and Class Members had a reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

72. Plaintiffs and Class Members relied on the Defendants to keep their PII and PHI confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

73. Plaintiffs and Class Members disclosed their PII and PHI and/or permitted Defendants to collect and store that information in an environment of privacy and confidentiality, and with the reasonable expectation that Defendants would protect that information, entailing Defendants' fiduciary obligations of confidentiality.

74. Plaintiffs and Class Members revealed their PII and PHI to Defendants with the understanding, whether express or implicit, that Defendants would keep the information confidential and secure and would not share or disclose it without their explicit authorization and without compliance with HIPAA obligations.

75. Plaintiffs and Class Members reasonably relied on Defendants' superior knowledge, skill, and sophistication to safeguard the confidentiality and integrity of their PII and PHI. Indeed, no reasonable person, including Plaintiffs and Class Members, would have provided their PII and PHI to Defendants, or allowed Defendants to collect and store such information without an understanding that Defendants would take reasonable steps to protect that information

consistent with their representations, their legal obligations, and the implied terms of their express contracts.

The Data Breach

76. On May 26, 2023, MCNA Dental confirmed they had suffered a ransomware attack that disrupted their computer systems. MCNA Dental purportedly detected the attack on March 6, 2023, blocked the unauthorized access, and launched an investigation to determine the nature and scope of the breach.

77. MCNA Dental confirmed that the hackers gained access to part of its systems and removed copies of Personal Information between February 26, 2023, and March 7, 2023. MCNA Dental concluded that the Data Breach impacted over 8,923,662 people, encompassing patients, parents, guardians, and/or guarantors.

78. The stolen information included names, addresses, dates of birth, emails, social security numbers, driver's license numbers and/or other government-issued ID numbers, health insurance information (plan information, insurance company, member number, Medicaid/Medicare ID numbers), care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment), and bills and insurance claims. Some of the stolen information was for a parent, guardian, or guarantor. Complimentary identity theft protection services were offered to individuals for one year.

79. Plaintiffs and other class members received a letter dated May 26, 2023 (the "Notice Letter"), stating *inter alia*:

> **What Happened?** On March 6, 2023, MCNA became aware that an unauthorized party was able to access certain MCNA systems. Upon discovery the same day, MCNA took immediate steps to contain the threat and engaged a third-party

> forensic firm to investigate the incident and assist with remediation efforts. MCNA subsequently discovered that certain systems within the network may have been infected with malicious code. Through its investigation, MCNA determined that an unauthorized third party was able to access certain systems and remove copies of some personal information between February 26, 2023 and March 7, 2023. MCNA undertook an extensive review to determine what data may have been impacted. As a result of this review, which was completed on May 3, 2023, it appears that your personal information may have been involved.
>
> **What information was involved?** Personal information that may have been involved included: (1) demographic information to identify and contact you, such as full name, date of birth, address, telephone and email; (2) Social Security number; (3) driver's license number or government-issued identification number; (4) health insurance information, such as name of plan/insurer/government payor, member/Medicaid/Medicare ID number, plan and/or group number; and (5) information regarding dental/orthodontic care. **Not all data elements were involved for all individuals.**
>
> **What we are doing**. MCNA takes privacy and security very seriously. As soon as we discovered the incident, we promptly launched a forensic investigation, took steps to mitigate and remediate the incident and to help prevent further unauthorized activity, and contacted law enforcement. In response to this incident, we have enhanced our security controls and monitoring practices as appropriate, to minimize the risk of any similar incident in the future.

80. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took approximately ten weeks to inform impacted individuals after Defendants determined their information was involved, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII and PHI remain protected. Moreover, Not every impacted individual will receive a notice, as MCNA Dental does not have current addresses for everyone. Accordingly, the organization published a substitute notice on IDX, which will stay online for 90 days. On that notice, MCNA

Dental identified a list of over a hundred healthcare providers indirectly impacted by this incident. It is unclear if those entities will publish separate notices.

81. Defendants' "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

82. The cyber attackers accessed and acquired files in Defendants' computer systems containing inadequately encrypted or unencrypted PII and PHI of Plaintiffs and Class Members, including their names, Social Security numbers, and health and/or clinical information. Accordingly, Plaintiffs' and Class Members' PII and PHI was accessed and stolen in the Data Breach.

The Data Breach Was Foreseeable and Preventable

83. Based on the type of customer patient PII and PHI Defendants collect, store and disseminate, Defendants know, or should have known, of the likelihood of a ransomware or other cyberattack or data breach of their information technology and data storage systems.

84. Ransomware attacks are frequently used to target healthcare providers due to the sensitive patient data they maintain. Attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network. Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in significant delays in services and accompanying disclosures of PII and PHI.

85. Ransomware attacks must be considered like other data breach incidents because ransomware attacks don't just hold networks hostage. Rather, "ransomware groups sell stolen data

in cybercriminal forums and dark web marketplaces for additional revenue."[9] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

86. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[10] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[11] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[12] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[13]

87. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.25 For example, such can be sold at a price ranging from $40 to $200. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

88. Social Security numbers, which were compromised in the Data Breach, are among the worst kind of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

89. The existence and prevalence of "Fullz" packages means that the PII and PHI stolen from the Data Breach can be linked to unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members, enabling cyber criminals to easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers). This makes the PII

and PHI compromised in the Data Breach significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, names, and health information.

90. Here, the PII and PHI data MCNA collected and maintained demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market." Accordingly, cyber criminals regularly target healthcare companies, like Defendants, due to the highly sensitive and valuable nature of the information they collect and maintain.

91. Defendants knew and understood that the PII and PHI they collect and maintain is valuable and highly sought after by cyber criminals who seek to illegally monetize that information through unauthorized access and theft.

92. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII and PHI, like Defendants, preceding the date of the breach.

93. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

94. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March

2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

95. Cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII and PHI are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[15]

96. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[14]

97. To prevent and detect cyber/ransomware attack and Data Breach Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

98. To prevent and detect the cyber/ransomware attack and Data Breach, Defendants also could and should have implemented, as recommended by the Microsoft Threat Protection

Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[16]

99. Had Defendants adequately and fully implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced.

100. Defendants could have prevented or detected the Data Breach prior to the hackers accessing Defendants' systems and extracting sensitive and personal information; the amount

and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former patients of Defendants would have been notified sooner, allowing them to promptly take protective and mitigating actions.

101. Upon information belief, Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII and PHI, such as encrypting the information or deleting it when it is no longer needed.

102. Upon information belief, Defendants did not comply with HIPAA, FTC or cybersecurity industry standards to protect its customer patients' PII and/or PHI, including such information of Plaintiffs and Class Members.

103. But for Defendants' failures, Plaintiffs' and Class Members' PII and PHI would not have been exposed to the Data Breach and stolen.

PLAINTIFFS' EXPERIENCE WITH DEFENDANTS

104. Plaintiff Nieblas formerly worked in the healthcare industry for over 15 years, with full knowledge of HIPAA requirements and guidance. Given her experience, Ms. Nieblas is highly knowledgeable about the importance of preventing unauthorized access to a patient's PHI and PII, particularly regarding the requirements of HIPAA.

105. Within the last several years, Plaintiff Nieblas obtained dental/ medical/ laboratory services, using her MCNA insurance through which Defendants were necessarily provided with her PII and PHI and which Defendants maintained.

106. At the time of the Data Breach, Defendants were in the possession, custody and control of Plaintiff Nieblas PII and PHI data in their computer system.

107. Plaintiff Nieblas is, and has been, very careful about sharing any of her PII and PHI,

stores any documents containing her PII and PHI in a safe and secure location and has never knowingly transmitted unencrypted PII or PHI to any unauthorized third party or over the internet or any other unsecured source.

108. Plaintiff Nieblas "feels that HIIPAA was violated" and is "incredibly concerned about [her] credit safety."

109. On or about June 13, 2023, Ms. Nieblas received MCNA's Notice Letter by U.S. mail. The Notice Letter did not provide any details of what specific information was taken from her and did not include any offer for credit monitoring.

110. Following knowledge regarding Defendants' Data Breach, Ms. Nieblas received "continuing Spam, 24/7, all of a sudden."

111. Plaintiff Nieblas was so concerned about the safety of her information that she immediately closed her existing bank account as a precautionary measure and took remedial steps in an attempt to identify what data was stolen from her.

112. In fact, in a follow up appointment following surgery two months prior to the Data Breach, the medical facility could not access Ms. Neiblas's existing medical records, nor would they prescribe her existing medication as a result of the Data Breach.

113. Plaintiff Nieblas suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of her privacy; (ii) loss of benefit of her bargain with Defendants when using their medical/laboratory services/products; (iii) lost time she spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminished value to her PII; and (vi) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access

and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect her PII and PHI.

114. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Nieblas has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach to verify the incident, attempting to obtain more details directly from the community hospital as to the extent of data taken, contacting credit reporting agencies, and has undertaken efforts on numerous social media accounts and her email account to gain access and change her passwords, including changing her email address, deleting accounts and changing passwords for social media accounts and her bank account.

115. Plaintiff Nieblas has spent significant time on these pursuits attempting to mitigate her damages from the data breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

116. Plaintiff Nieblas is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come. Accordingly, Plaintiff Nieblas anticipates spending considerable time and money on an ongoing basis to try to mitigate and address future harms caused by the Data Breach.

117. The Data Breach has caused Plaintiff Nieblas to suffer anxiety and stress, including her fear of additional unknown repercussions, all of which has been compounded by the fact that Defendants have still not fully informed her of the key details about the Data Breach's occurrence or bothered to offer her credit monitoring.

118. Plaintiff Nieblas has a continuing interest in ensuring that her PII and PHI, which,

upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

119. Plaintiff Jane Doe is Plaintiff Neiblas's 13-year-old daughter and has experienced the same attendant issues as her mother, Plaintiff Neiblas.

120. Plaintiff Jane Doe received her Notice Letter at the same time as Plaintiff Neiblas, and Plaintiff Nieblas suffers the same concerns and anxiety with respect to her minor child Jane Doe's experiences with the Data Breach, including consistent reporting and monitoring of all accounts.

121. Plaintiff Jane Doe suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of her privacy; (ii) loss of benefit of her bargain with Defendants when using their medical/laboratory services/products; (iii) diminished value to her PII; and (vi) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect her PII and PHI.

122. Plaintiff Jane Doe is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

PLAINTIFFS' AND CLASS MEMBERS' COMMON INJURIES

123. As a result of the Data Breach and Defendants' related failures to adequately protect their customer patients' PII and PHI information, Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred

mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (i) the continued risk to their PII and PHI, which remain in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' confidential information.

124. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes.

125. The unencrypted PII and PHI of Plaintiffs and Class Members will be available for sale on the dark web as that is the *modus operandi* of hackers, as already has been experienced by Plaintiffs.

126. Unencrypted PII and PHI of Plaintiffs and Class Members may also fall into the hands of unauthorized individuals and companies that will use such information for targeted marketing without the approval of Plaintiffs and Class Members.

127. As a consequence of the Data Breach, Plaintiffs and Class Members must take time to learn about the breach and are expected to take reasonable steps to mitigate injuries including, but not limited to, researching the Data Breach to verify the incident and obtain more details on its occurrence, monitoring their financial accounts and monitoring their credit files with the credit reporting agencies, contacting one of the credit bureaus to place a fraud alert, contacting companies

to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

128. According to a 2022 Consumer Impact Report by the Identity Theft Resource Center, available at https://www.idtheftcenter.org/publications/, victims of data breaches/cyber theft have experienced numerous types of harm, including financial injuries, the expenditure of time to resolve id theft and credit issues, and emotional/psychological injuries, with total financial value of such injuries exceeding $500 for 65% of all victims.

129. Given the nature and extent of PII and PHI data MCNA collects, stores and disseminates for its customer patients, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize Plaintiffs' and Class Members' PII and PHI for identity theft crimes, including, e.g., opening credit cards or taking out loans in their name; filing false income tax returns and intercepting refunds; and filing false unemployment claims.

130. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

131. Because fraudulent activity involving Plaintiffs' and Class Members' PII and PHI resulting from the Data Breach may not come to light for years, Plaintiffs and Class Members will be required to maintain constant surveillance of their financial and personal records for years to come.

132. In addition, Plaintiffs' and Class Members' right to their PII and PHI are valuable

property rights. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[17]

133. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[18] The data marketplace even enables consumers to sell their non-public information to data brokers who in turn aggregate such information and re-sell it to marketers and app developers, including the Nielsen Corporation.[19]

134. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, their PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

135. Plaintiffs and Class Members will need credit and identity theft monitoring for a minimum of five years to protect their identities as a result of the Data Breach. The retail cost of such monitoring can run approximately $200 a year per Class Member. Such costs are reasonable and necessary to protect Class Members from the risk of identity theft.

136. Defendants' failure to protect Plaintiffs' and Class Members' PII and PHI deprived them of the benefit of their bargain with Defendants when paying for Defendants' medical and laboratory products and services.

137. When agreeing to pay Defendants for such medical and laboratory services and products, Plaintiffs and Class Members understood and expected that they were, in part, paying for the service and necessary data security to protect their PII and PHI, when in fact, Defendants did not provide the expected data security. Accordingly, the products and services that Plaintiffs

and Class Members received from Defendants were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

CLASS ACTION ALLEGATIONS

138. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

139. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose PII and/or PHI was maintained on Defendants' computer systems that were compromised in the Data Breach reported by Defendants in May 2023 (the "Class").

140. Excluded from the Class are Defendants, officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

141. Plaintiffs hereby reserve the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

142. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, it has been reported that the Class consists of approximately 8.9 million persons whose data was compromised in Data Breach.

143. There are questions of law and fact common to the Class that predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, provided access to, or disclosed Plaintiffs' and Class Members' PII and PHI;

b. Whether Defendants failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the PII and PHI compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Plaintiffs and Class Members to safeguard their PII and PHI;

f. Whether Defendants breached their duties to Plaintiffs and Class Members to safeguard their PII and PHI;

g. Whether computer hackers obtained Plaintiffs' and Class Members' PII and PHI in the Data Breach;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants breached implied contracts for adequate data security with Plaintiffs and Class Members;

l. Whether Defendants were unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members;

m. Whether Defendants failed to provide adequate notice of the Data Breach in a timely manner; and,

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

144. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII and PHI, like that of every other Class Member, was compromised in the Data Breach.

145. Adequacy of Representation. Plaintiffs will fairly and adequately represent and

protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

146. Predominance. Defendants have engaged in a common course of conduct to and Class Members, in that all the Plaintiffs' and Class Members' PII and PHI was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Plaintiffs and Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

147. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

148. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

149. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which

would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PII and PHI;

b. Whether Defendants' security measures to protect its data systems were compliant with HIPAA and FTC requirements;

c. Whether Defendants' security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants failed to take reasonable and appropriate steps to safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether Defendants' failure to institute adequate protective security measures amounted to negligence; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

150. Finally, all Members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendant MCNA.

CAUSES OF ACTION

Count I – Negligence
(On Behalf of Plaintiff and All Class Members)

151. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 150 as if fully set forth herein.

152. Defendants require their customer patients, including Plaintiffs and Class Members, to submit non-public PII and PHI in the ordinary course of providing its medical/laboratory products and services.

153. Defendants gathered and stored the PII and PHI of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' patients, which solicitations and services affect commerce.

154. Plaintiffs and Class Members entrusted Defendants with their PII and PHI with the understanding that Defendants would safeguard their information.

155. Defendants had full knowledge of the sensitivity of Plaintiffs' and Class Members' PII and PHI, as well as the types of harm that Plaintiffs and Class Members could and would suffer if their PII and PHI were wrongfully disclosed.

156. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII and PHI held within it—to prevent unauthorized access and disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

157. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

158. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the

healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

159. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

160. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and its customer patients. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII and PHI, a necessary part of being customer patients of Defendants.

161. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII and PHI.

162. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

163. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customer patients' PII and PHI that it was no longer required to retain pursuant to regulations.

164. Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

165. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and Class Members within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised

and when. Such notice is necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their confidential information by third parties.

166. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' PII and PHI;

b. Failing to adequately monitor the security of, and secure, their networks and systems;

c. Allowing unauthorized access to, and the theft of, Plaintiffs' and Class Members' PII and PHI;

d. Failing to detect in a timely manner that Plaintiffs' and Class Members' PII and PHI had been compromised;

e. Failing to remove former customer patients' PII and PHI it was no longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Plaintiffs and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

167. Defendants violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII and PHI it obtains, stores and disseminates in the ordinary course of its business and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members if that data was accessed and stolen.

168. Plaintiffs and Class Members are within the class of persons that the FTC Act and HIPAA were intended to protect.

169. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

170. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

171. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of the nature of Defendants' business and its inadequate security practices.

172. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

173. Defendants have full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if their PII and PHI were wrongfully disclosed.

174. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures.

175. Defendants knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting such information stored on Defendants' computer systems and network.

176. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs' and

Class Members' PII and PHI would result in one or more types of injuries to Plaintiffs and Class Members.

177. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in, and possibly remains in, Defendants' possession.

178. Defendants were in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

179. Defendants' duty extended to protecting Plaintiffs and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

180. Defendants have admitted that the PII and PHI of Plaintiffs and Class Members was wrongfully accessed by cybercriminals and potentially lost and disclosed to unauthorized third persons as a result of the Data Breach.

181. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII and PHI of Plaintiffs and Class Members would not have been compromised.

182. There is a close causal connection between Defendants' failure to implement security measures to protect the PII and PHI Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The PII and PHI of Plaintiffs and the Class were accessed and stolen as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such information by adopting, implementing, and maintaining

appropriate security measures.

183. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time, spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) the diminished value of their PII and PHI, and (vi) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect that information.

184. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

185. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect such information in their continued possession.

186. Defendants' negligent conduct is ongoing, in that it still holds the PII and PHI of Plaintiffs and Class Members in an unsafe and insecure manner.

187. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

188. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

Count II – Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

189. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 150 as if fully set forth herein.

190. Plaintiffs and Class Members were required to provide their PII and PHI to Defendants as a condition of, and a necessary part of, receiving medical/laboratory products and services from Defendants.

191. Plaintiffs and Class Members entrusted their PII and PHI to Defendants. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

192. Implicit in the agreement between Plaintiffs and Class Members on the one hand, and the Defendants on the other hand, to provide their PII and PHI, Defendants were obligated to: (a) use such PII and PHI for authorized business purposes only, (b) take reasonable steps to safeguard that information, (c) prevent unauthorized disclosures of the information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI, (e) reasonably safeguard and protect the PII and PHI of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII and PHI only under conditions that kept such information secure and confidential.

193. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

194. Defendants solicited, offered, and invited Plaintiffs and Class Members to provide their PII and PHI, and enable Defendants to collect, maintain and disseminate such information, as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their PII and PHI to Defendants.

195. In accepting the PII and PHI of Plaintiffs and Class Members, Defendants understood and agreed that they were required to reasonably safeguard that information from unauthorized access or disclosure.

196. At all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose PII and PHI under certain circumstances, none of which relate to the Data Breach.

197. Defendants implicitly promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII and PHI would remain protected.

198. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

199. Plaintiffs and Class Members paid money to Defendants with the reasonable belief and expectation that Defendants would use part of its earnings to obtain adequate data security. Defendants failed to do so.

200. Plaintiffs and Class Members would not have entrusted their PII and PHI to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

201. Plaintiffs and Class Members would not have entrusted their PII and PHI to Defendants in the absence of Defendants' implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

202. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

203. Defendants breached the implied contracts they made with Plaintiffs and Class Members by failing to safeguard and protect their PII and PHI, by: (a) failing to delete such information once the relationship ended, and (b) by failing to provide adequate notice to them that personal information was compromised as a result of the Data Breach.

204. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

205. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

Count III – Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

206. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 150 as if fully set forth herein.

207. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for services from Defendants and/or their agents and in so doing provided Defendants with their PII and PHI. In exchange, Plaintiffs and Class Members should have received from Defendants the medical/laboratory services and products that were the subject of the transaction and should have had their PII and PHI protected with adequate data security.

208. Defendants knew that Plaintiffs and Class Members conferred a benefit on them in

the form their PII and PHI, as well as payments made on their behalf as a necessary part of their receiving healthcare services. Defendants appreciated and accepted that benefit. Defendants profited from these transactions and used the PII and PHI of Plaintiffs and Class Members for business purposes.

209. Upon information and belief, Defendants fund their data security measures entirely from its general revenue, including payments on behalf of or for the benefit of the medical/laboratory products and services that Defendants provide to Plaintiffs and Class Members.

210. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

211. Defendants, however, failed to secure Plaintiffs' and Class Members' PII and PHI and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided to Defendants.

212. Defendants would not be able to carry out an essential function of their regular business without the PII and PHI of Plaintiffs and Class Members and derived revenue by using that information for its business purposes. Plaintiffs and Class Members expected that Defendants or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

213. Defendants acquired the PII and PHI through inequitable means in that they failed to disclose the inadequacy of their security practices to Plaintiffs and Class Members. If Plaintiffs and Class Members knew that Defendants had not reasonably secured their PII and PHI, they would not have allowed their PII and PHI to be provided to Defendants.

214. Defendants enriched themselves by saving the costs it reasonably should have

expended on data security measures to secure Plaintiffs' and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security and the safety of their PII and PHI.

215. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

216. Plaintiffs and Class Members have no adequate remedy at law.

217. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) loss of benefit of the bargain; (iii) lost time, spent on activities remedying harms resulting from the Data Breach; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) diminished value of their PII; and (vi) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and PHI.

218. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class

Members have suffered and will continue to suffer other forms of injury and/or harm.

219. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' products and services.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the PII and PHI of

Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' computer systems and network on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' computer systems

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the PII and PHI of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its

respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

Dated: June 23, 2023

Respectfully submitted,

/s/ Nicholas A. Colella
Gary F. Lynch
Nicholas A. Colella
LYNCH CARPENTER, LLP
1133 Penn Ave., Fl. 5
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
nickc@lcllp.com

James M. Evangelista
EVANGELISTA WORLEY LLC
500 Sugar Mill Road Suite 245A
Atlanta, GA 30350
Tel.: 404-205-8400
Fax: 404-205-8395
Email: jim@ewlawllc.com

Jennifer Czeisler
JKC LAW, LLC
269 Altessa Blvd.
Melville, NY 11747
Tel: (516)457-9571
Email: jennifer@jkclawllc.com

Attorneys for Plaintiffs